UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/700,786	11/03/2003	Mariusz H. Jakubowski	MS1-1664US	5484

22801 7590 12/23/2008

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/700,786	JAKUBOWSKI ET AL.	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-15,32,36-38,56-58 and 63-71* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-15,32,36-38,56-58 and 63-71* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9, 11-15, 32, 36-38, 56-58 and 63-71 are pending in this application.

2. Claims 1, 3-5, 7, 32, 37 and 56-57 are currently amended.

3. Claims 10, 16, 33-35, 39 and 59-62 are cancelled.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Claim Rejections - 35 USC § 103

5. Claims 32, 36, 38, 57-58 and 63-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener et al. (Pub. No.: US 2003/0105980 A1), hereinafter "Challener" and further in view of Bailey (Patent No.: US 7,205,883 B2).

6. As to claim 32, Challener discloses a computer readable medium having stored thereon computer executable instructions for performing acts comprising:

accessing a user key associated with a user ID, wherein the accessing is from a user key data structure and is upon presentation of a user ID of a user (FIG. 1, which maintains a data structure of plurality of users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password; [0019]),

hashing, upon presentation of a password of the user, the presented password, to thereby produce a hash value (FIG. 1, which maintains a data structure of plurality of

users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password; [0019]);

Although Challener discloses a data structure comprising plurality of users with different hash value as key associated with one of a plurality of users (FIG. 1), Challener doesn't explicitly disclose the plurality of encryptions of the master key is associated with one of a plurality of users, respectively, and wherein each of the plurality of encryptions of the user master key was encrypted by operation of a reversible process using a hash value of a password of an associated user as a key in the reversible process; decrypting the user key using the hash value, thereby creating the master decrypting data using the master key.

However, Bailey discloses wherein the encryptions of the user master key was encrypted by operation of a reversible process using a hash value of a password of an associated user as a key in the reversible process (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K"); decrypting the user key using the hash value, thereby creating the master decrypting data using the master key (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to public network.

7. As to claim 57, it is rejected using the same rationale as for the rejection of claim 32.

8. As to 58, Challener doesn't explicitly disclose having further computer executable instructions for performing acts of: delivering the data structure to one or more of the plurality of users. However, Bailey discloses delivering the data structure to one or more of the plurality of users (col. 8, lines 7-25, which describes that the keys are transmitted to the host site).

9. As to claims 36 and 63, Challener discloses wherein each user key includes an integrity verification feature ([0019], "The phrase signed with the loaded private key is then compared with the stored signed phrase associated with the remote user…").

10. As to claims 38 and 64, Challener discloses wherein each user key includes a checksum ([0002], [0019]).

11. Claims 37 and 65-70 are unpatentable over Challener and further in view of Bailey and Thomlinson et al. (Patent No.: US 6,272,631 B1), hereinafter "Thomlinson".

12. As to claim 37, neither Challener nor Bailey explicitly discloses wherein the master key includes an integrity verification feature. However, Thomlinson discloses wherein the master key includes an integrity verification feature (col. 10, lines 30-65,

"The master authentication key is used in conjunction with the specified MAC to verity that the master key decrypted correctly").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifyi8ng the remote user's identity.

13. As to claims 65, neither Challener nor Bailey explicitly discloses wherein each user key includes a keyed-hash message authentication code. However, Thomlinson discloses a user key comprising a master key and a keyed-hash message authentication code (FIG. 3, lines 30-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

14. As to claim 66, neither Challener nor Bailey explicitly discloses transforming data using the master key. However, Thomlinson discloses transforming data using the master key (column 10, lines 30-65, "The master key is then used to decrypt an appropriate item key...").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

15. As to claim 67, neither Challener nor Bailey explicitly disclose storing data transformed using the master key; and controlling access by the plurality of users to the transformed data. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and controlling access by the plurality of users to the transformed data (column 9, lines 50-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

16. As to claim 68, Challener discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]). Neither Challener nor Bailey explicitly discloses storing data transformed using the master key; and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 50-67 and column 10, lines 1-10); and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

17. As to claim 69, Challener discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]). Neither Challener nor Bailey explicitly discloses storing data transformed using the master key; and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 50-67 and column 10, lines 1-10); and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

18. As to claim 70, Challener discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]); selecting a user key from the data structure based on the received user id (FIG. 1, [0019], [0021]). Challener doesn't explicitly disclose storing data transformed using the master key; decrypting the selected user id using the received password to reproduce the master key; and using the master key to access the data.

However, Bailey discloses decrypting the selected user id using the received password to reproduce the master key (FIG. 4, column 8, lines 7-25, "..K-unwrapping of [SAK].sub.K.").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to a network.

Neither Challener nor Bailey explicitly discloses storing data transformed using the master key; and using the master key to access the data.

However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and using the master key to access the data (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

19. Claims 1-9, 11-15, 56 and 71 are unpatentable over Challener and further in view of Bailey, Thomlinson Claim 71 and Tewfik et al. (Pub. No.: US 2003/0095685 A1), hereinafter "Tewfik".

20. As to claim 1, Challener discloses a method comprising:

creating a data structure including a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users (FIG. 1, which maintains a data structure of plurality of users and with hash of user password; it

should be noted that hash value for each of the user password is different and reversible by each user's password; [0019]**);**

receiving a user id and user password from one of the plurality of users (FIG. 1, [0019], [0021]);

selecting a user key from the data structure based on the received user id (FIG. 1, [0019], [0021]);

hashing the received password to produce a hash value (FIG. 1, [0002]);

Although Challener discloses a data structure comprising plurality of users with different hash value as key associated with one of a plurality of users (FIG. 1), Challener doesn't explicitly disclose a user key comprising a master key and a keyed-hash message authentication code encrypted using a password associated with the one of the plurality of users; storing data watermarked using the master key; decrypting the selected user key using the hash value to reproduce the master key; using the master key to access the watermarked data; and delivering the data structure to one or more of the plurality of users.

However, Bailey discloses a user key comprising a master key using a password associated with the one of the plurality of users (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K"); decrypting the selected user key using the hash value to reproduce the master key; using the master key to access the watermarked data (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K"); and

delivering the data structure to one or more of the plurality of users (col. 8, lines 7-25, wherein key is being transmitted to the host sites).

Although keyed has message authentication code for integrity verification is well known in the art, neither Challener nor Bailey explicitly disclose a keyed-hash message authentication code encrypted using a password; storing data watermarked using the master key.

However, Thomlinson discloses disclose a keyed-hash message authentication code encrypted using a password (FIG. 3, col. 9, lines 30-57); storing data using the master key (and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

Neither Challener and Bailey nor Thomlinson explicitly discloses watermarked data. However, Tewfik discloses watermarked data ([0015], [0020]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener, Bailey and Thomlinson as taught by Tewfik in order to protect contents from unauthorized duplication.

21. As to claim 56, it is rejected using the same rationale as for the rejection of claim 1.

22. As to claim 2, Challener doesn't explicitly disclose wherein the act of delivering comprises delivering the data structure to each of the plurality of users. However, Bailey discloses wherein the act of delivering comprises delivering the data structure to each of the plurality of users (column 8, lines 7-25, "The [SAK].sub.K is transmitted to the host site...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to support multiple users in password-based access to a network.

23. As to claim 3, Challener discloses a hash of the password associated with the one of the plurality of users (FIG. 1, [0002]). Challener doesn't explicitly disclose wherein each master key is encrypted using a hash of the password. However, Bailey discloses wherein each master key is encrypted using a hash of the password (FIG. 4, column 8, lines 7-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to a network.

24. As to claims 4 and 5, these are rejected using the same rationale as for the rejection of claim 3.

25. As to claim 6, Challener discloses wherein each user key has an integrity verification feature associated therewith ([0019], "The phrase signed with the loaded private key is then compared with the stored signed phrase associated with the remote user..").

26. As to claims 7 and 8, neither Challener nor Bailey explicitly discloses wherein each master key has an integrity verification feature associated therewith. However, Thomlinson discloses wherein each master key has an integrity verification feature associated therewith (column 10, lines 30-65, "The master authentication key is used in conjunction with the specified MAC to verity that the master key decrypted correctly").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

27. As to claim 9, Challener discloses wherein each user key includes a checksum ([0002], [0019]).

28. As to claim 11, neither Challener nor Bailey explicitly discloses transforming data using the master key. However, Thomlinson discloses transforming data using the master key (column 10, lines 30-65, "The master key is then used to decrypt an appropriate item key...").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

29. As to claim 12, neither Challener nor Bailey explicitly disclose storing data transformed using the master key; and controlling access by the plurality of users to the transformed data. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and controlling access by the plurality of users to the transformed data (column 9, lines 50-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

30. As to claim 13, Challener discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]). Neither Challener nor Bailey explicitly discloses storing data transformed using the master key; and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password. However, Thomlinson discloses storing data transformed using the master key (column 9, lines 50-67 and column 10, lines 1-10); and controlling access to the transformed data by the one of the plurality of users based on the received user id and user password (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

31. As to claim 14, these are rejected using the same rationale as for the rejection of claim 13.

32. As to claim 15, Challener discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]); selecting a user key from the data structure based on the received user id (FIG. 1, [0019], [0021]). Challener doesn't explicitly disclose storing data transformed using the master key; decrypting the selected user id using the received password to reproduce the master key; and using the master key to access the data.

However, Bailey discloses decrypting the selected user id using the received password to reproduce the master key (FIG. 4, column 8, lines 7-25, "..K-unwrapping of [SAK].sub.K.").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to a network.

Neither Challener nor Bailey explicitly discloses storing data transformed using the master key; and using the master key to access the data.

However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and using the master key to access the data (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

33. As to claim 71, Challener discloses receiving a user id and user password from one of the plurality of users ([0019], [0021]); selecting a user key from the data structure based on the received user id (FIG. 1, [0019], [0021]). Hashing the received password to produce a hash value (FIG. 1, [0002]). Challener doesn't explicitly disclose storing data watermarked using the master key; decrypting the selected user id using the received password to reproduce the master key; and using the master key to access the watermarked data.

However, Bailey discloses decrypting the selected user id using the received password to reproduce the master key (FIG. 4, column 8, lines 7-25, "..K-unwrapping of [SAK].sub.K.").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to a network.

Neither Challener nor Bailey explicitly discloses storing data watermarked using the master key; and using the master key to access the watermarked data.

However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and using the master key to access the data (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

Neither Challener and Bailey nor Thomlinson explicitly discloses watermarked data. However, Tewfik discloses watermarked data ([0015], [0020]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener, Bailey and Thomlinson as taught by Tewfik in order to protect contents from unauthorized duplication.

34. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Arguments

35. Applicant has amended claims 1, 3-5, 7, 32, 37 and 56-57, which necessitated new rejection, please see rejection above. Applicant's arguments filed September 30th, 2008 have been fully considered but they are not persuasive.

36. In response to claim 1, Applicant argues that: "Challener fails to teach or suggest a table which associates each user with a different encrypted version of the master password, available to each of a plurality of users, and particularly wherein such a version was encrypted with the hash of the user's password".

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "a table with associated each user with a different encrypted version of the master password") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Challener maintains a data structure of plurality of users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password, e.g. see, FIG. 1, [0019].

37. Applicant argues that: "Bailey fails to teach or suggest a table which associates each user with a different encrypted version of the master password, available to each

of a plurality of users, and particularly wherein such a version was encrypted with the hash of the user's password".

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "a table with associated each user with a different encrypted version of the master password") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Challener maintains a data structure of plurality of users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password, e.g. see, FIG. 1, [0019].

38. Applicant argues that: "Thomlinson fails to teach or suggest a table which associates each user with a different encrypted version of the master password, available to each of a plurality of users, and particularly wherein such a version was encrypted with the hash of the user's password."

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "a table with associated each user with a different encrypted version of the master password") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore,

Challener maintains a data structure of plurality of users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password, e.g. see, FIG. 1, [0019].

39. Applicant argues that: "Applicant submits that none of the art teaches or suggests that a single password (e.g. the "master password") is encrypted in a plurality of different ways, and is thereby made available to a plurality of different users."

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "a single password (e.g. the "master password") is encrypted in a plurality of different ways, and is thereby made available to a plurality of different users.") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Challener maintains a data structure of plurality of users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password, e.g. see, FIG. 1, [0019]. Bailey discloses a user key comprising a master key using a password associated with the one of the plurality of users (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K").

40. In response to claim 32, Applicant argues that: "...none of the art teaches or suggest a "plurality of encryptions of the master key is associated with one of a plurality of users, respectively."

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Furthermore, Challener discloses a data structure comprising plurality of users with different hash value as key associated with one of a plurality of users (FIG. 1 and Bailey discloses wherein the encryptions of the user master key was encrypted by operation of a reversible process using a hash value of a password of an associated user as a key in the reversible process (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K").

41. Applicant argues that: "The prior art fails to teach or suggest such multiple different encryptions of a key, generally, and more specifically, associating each of the encryptions of master key with one of a plurality of users"

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "multiple different encryptions of a key, generally, and more specifically, associating each of the encryptions of master key with one of a plurality of users") are not recited in the rejected claim(s). Although the claims are interpreted in light of the

specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Challener maintains a data structure of plurality of users and with hash of user password; it should be noted that hash value for each of the user password is different and reversible by each user's password, e.g. see, FIG. 1, [0019]. Bailey discloses a user key comprising a master key using a password associated with the one of the plurality of users (FIG. 4, col. 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K").

Conclusion

42. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435